Claims

1) A method of producing a system architecture comprising a plurality of electrical devices connected to each other, said system preferably comprising a fault tolerant system, the method including:

a) identifying a set of undesirable events and ascribing to each of said undesirable events an indicator of their severity;

b) associating where possible each said undesirable event with one or more actuators of said system architecture;

c) developing a functional specification of an initial architecture proposed for implementation of said system architecture, said functional specification of said initial architecture including dataflow for and between components thereof, said components comprising for example sensors or actuators;

d) refining on said functional specification the fault tolerance requirements associated with the severity of each said undesirable event and issuing refined fault tolerance requirements of said functional specification;

e) producing replicates in said functional specification together with attached indicators of independence of said replicates, said indicators reflecting said refined fault tolerance requirements;

f) defining a hardware structure for said system architecture, e.g. a series of electronic control units connected to each other by networks;

g) mapping of said functional specification onto said hardware structure; and

h) verifying automatically that said indicators of independence are preserved during mapping.

2) A method according to claim 1, including, preferably in step (c), defining a series of modes of operation, e.g. nominal and limp-home modes.

3) A method according to claim 2, including specifying said series of modes in the form of one or more state charts.

4) A method according to any preceding claim, including mapping geometrically hardware components and/or wiring and then verifying automatically that said indicators of independence are preserved by said geometrical mapping.

5) A method according to any preceding claim, including specifying severity in the form of probability of failure per unit of time.

6) A method according to any preceding claim, including outputting a set of data for manufacturing said system architecture.

7) A method according to any preceding claim, wherein said architecture comprises an architecture for a vehicle, for example a safety critical architecture such as control circuitry for a brake system.

8) A computer program product comprising a computer readable medium having thereon computer program code means, when said program is loaded, to make the computer execute procedure to design and verify a system architecture, said procedure comprising:

a) identifying a set of undesirable events and ascribing to each of said undesirable events an indicator of their severity;

b) associating where possible each said undesirable event with one or more actuators of said system architecture;

c) developing a functional specification of an initial architecture proposed for implementation of said system architecture, said functional specification of said initial architecture including dataflow for and between components thereof, said components comprising for example sensors or actuators;

d) refining on said functional specification the fault tolerance requirements associated with the severity of each said undesirable event and issuing refined fault tolerance requirements of said functional specification;

e) producing replicates in said functional specification together with attached indicators of independence of said replicates, said indicators reflecting said refined fault tolerance requirements;

f) defining a hardware structure for said system architecture, e.g. a series of electronic control units connected to each other by networks;

g) mapping of said functional specification onto said hardware structure; and

h) verifying automatically that said indicators of independence are preserved during mapping.

9) A design tool adapted for the design and verification of a system architecture, said design tool being adapted to implements the steps of any one of claims 1 to 7, or programmed using a computer program product according to claim 8.